(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 April 2005 (28.04.2005)

PCT

(10) International Publication Number
WO 2005/038635 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number:
PCT/IB2004/002716

(22) International Filing Date: 20 August 2004 (20.08.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03405749.7 17 October 2003 (17.10.2003) EP
04405181.1 24 March 2004 (24.03.2004) EP

(71) Applicant *(for all designated States except US)*: INTERNATIONAL BUSINESS MACHINES CORPORATION [US/US]; New Orchard Road, Armonk, NY 10504 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: CAMENISCH, Jan [CH/CH]; Bahnhofstrasse 13, CH-8803 Rueschlikon (CH).

(74) Agents: TOLETI, Martin et al.; IBM Research GmbH, Zurich Research Laboratory, Saeumerstrasse 4 / Postfach, CH-8803 Rueschlikon (CH).

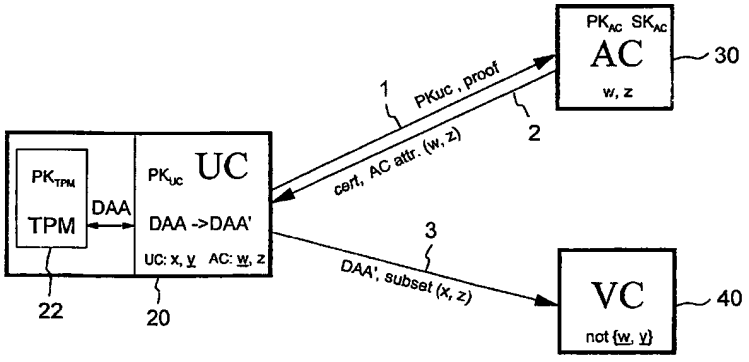
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR USER ATTESTATION-SIGNATURES WITH ATTRIBUTES



(57) Abstract: The present invention discloses a method for generating and verifying a user attestation-signature value (DAA') and issuing an attestation value (*cert*) for the generation of the user attestation-signature value (DAA'). Further, the invention is related to a system for using a user attestation-signature value (DAA') that corresponds to at least one attribute (A, B, C, D), each with an attribute value (w, x, y, z), none, one or more of the attribute values (x, y) remaining anonymous for transactions, the system comprising: a user device (20) having a security module (22) that provides a module public key (PK_{TPM}) and a security module attestation value (DAA), the user device (20) providing a user public key (PK_{UC}) that inherently comprises none, one, or more user determined attribute value (x, y) and a proof value demonstrating that the user public key (PK_{UC}) is validly derived from the module public key (PK_{TPM}) of the security module (22); an attester computer (30) that provides none, one, or more attester determined attribute value (w, z) and an attestation value (cert) that bases on an attester secret key (SK_{AC}), the user public key (PK_{UC}), and an anonymous attribute value (w, z); and a verification computer (40) for verifying whether or not (i) the user attestation-signature value (DAA') was validly derived from the security module attestation value (DAA) provided by the security module (22) and the attestation value (*cert*), and (ii) the attestation value (cert) is associated with a subset (B, D) of at least one attribute, each attribute in the subset (B, D) having a revealed attribute value (x, z).

WO 2005/038635 A2